LISTING OF THE CLAIMS:

1. (Previously presented) A method for protecting a computer network from vulnerabilities, comprising:

quarantining a computer system to said computer network by said computer system raising a firewall resident on the computer system whenever physically connecting or reconnecting said computer system until said quarantined computer system is remediated, wherein said quarantine of said computer system is self-initiated, and wherein said firewall allows specified permitted communications while blocking all other communications;

determining if the computer system requires remediation, wherein the determination is performed by a component of the computer network communicating with the computer system, and wherein the communication between the computer system and the component is one of the specified permitted communications;

remediating the computer system using information from the component of the computer network in accordance with the determination; and

upon completing remediation of said quarantined computer system, the computer system lowering the firewall to allow all communication between the computer system and the computer network.

2-4. (Canceled)

5. (Previously presented) The method of claim 1, wherein a specified permitted communication between the computer system and the component of the network includes a flow of vulnerability resolution information.

6. (Canceled)

7. (Currently Amended) For a computer network comprised of a plurality of computer systems and a client remediation server coupled to each one of said plurality of computer systems, said client remediation server remediating said computer network by resolving vulnerabilities in said plurality of computer systems, a method for protecting said remediated computer network from unresolved vulnerabilities, comprising:

if one of said computer systems of said remediated computer network is physically disconnected from said remediated computer network, ~~upon a~~ whenever subsequently physically re-connecting ~~re-connection of~~ said computer system to said remediated computer network, said computer system raising a firewall resident on the computer system to temporarily limit exchanges between said remediated computer network and said computer system until said computer system has been verified by said remediation server, wherein said computer system lowers the firewall upon said remediation server verifying said computer system.

8. (Previously presented) The method of claim 7, wherein the verification includes checking for pending remediations for said computer system.

9. (Canceled)

10. (Previously presented) The method of claim 7, wherein limiting exchanges between said remediated computer network and said computer system includes filtering out non-remediation-related traffic.

11. (Previously presented) The method of claim 8, wherein verifying said computer system includes said client remediation server executing said pending remediations for said computer system.

12. (Canceled)

13. (Previously presented) The method of claim 7, wherein lowering the firewall permits non-remediation-related traffic to pass between said computer system and said remediated computer network without filtering.

14. (Currently Amended) A method for protecting a computer network from nefarious software associated with a computer system being connected to said computer network, comprising:

~~upon~~ whenever initiating a connection between connecting said computer system and said computer network, said computer system quarantining itself from said computer network by raising a firewall resident on said computer system, wherein the firewall allows specified permitted communications related to protecting said computer network and blocks all other communications with said computer network over said connection;

performing a scan on said computer system with ~~information from~~ a component of said computer network; and

lifting said quarantine of said computer system by said computer system lowering the firewall upon completing a removal of any nefarious software detected by said scan.

15-17. (Canceled)

18. (Previously presented) The method of claim 14, wherein traffic between said computer system and said component of said computer network is related to said nefarious software detection and removal and is a specified permitted communication allowed to pass through the firewall.

19. (Original) The method of claim 18, wherein said nefarious software is a computer virus.

20. (Original) The method of claim 18, wherein said nefarious software is a worm.

21. (Currently Amended) A remediated computer network comprising:

a computer system; and

a client remediation server coupled to said computer system, said client remediation server configured to resolve vulnerabilities in said computer system whenever said computer system physically connects or reconnects to said computer network[[;]],

wherein said computer system includes a firewall for isolating said computer system from said remediated computer network ~~upon~~ whenever said computer system physically connects[[ing]] or reconnects[[ing]] to said computer network, until said client remediation server resolves vulnerabilities of said computer system, and

wherein resolving vulnerabilities in said computer system includes determining if said computer system has vulnerabilities.

22. (Currently Amended) The computer network of claim 21, wherein said computer system is configured to raise said firewall to isolate said computer system from said remediated computer network whenever said computer system disconnects from and subsequently ~~physically~~ reconnects to said computer network.

23. (Previously presented) The computer network of claim 22, wherein said computer system is configured to raise said firewall upon each power-up thereof.

24. (Previously presented) The computer network of claim 22, wherein said remediated computer network is a local area network (LAN) and said computer system is configured to raise said firewall upon initiating registration with said LAN.

25. (Previously presented) The computer network of claim 22, wherein said remediated computer network is a wide area network (WAN) and said computer system is configured to raise said firewall upon initiating registration with said WAN.

26. – 29. (Canceled)

30. (Currently Amended) A computer system, comprising:

a processor subsystem;

a memory subsystem coupled to said processor subsystem;

at least one application residing in said memory subsystem and executable by said processor subsystem; and

a firewall switchable between a closed position and an open position;

wherein said firewall is configured to switch into said closed position upon power-up of said computer system and upon initiation of registration with a computer network; and

wherein all traffic to and from said computer system is generally restricted when said firewall is switched to said closed position, and where said firewall permits specific access through said firewall including at least to locate and communicate with a remediation server of said computer network when said firewall is switched to said closed position; and

wherein the firewall is configured to switch from said closed position to said open position only upon said remediation server verifying that said computer system meets standards of said network.

31. (Canceled)

32. (Previously presented) The computer system of claim 30, wherein the specific access through the firewall to locate and communicate with said remediation server of

said computer network is the only specific access permitted through said firewall when said firewall is switched to said closed position.

33. (Previously presented) The computer system of claim 30, wherein communication with said remediation server includes traffic for executing pending remediations and traffic for executing supplementary remediations determined necessary by said client remediation server.

34. (Previously presented) The computer system of claim 30, wherein initiating registration with said computer network is initiated upon physically connecting said computer system with said computer network.

35. (Previously presented) The method of claim 1, wherein physically reconnecting the computer system to the computer network includes one of detaching a physical communication link between the computer system and the computer network and subsequently attaching the physical communication link or powering down the computer system while maintaining the physical communication link and subsequently powering up the computer system.

36. (Previously presented) The method of claim 35, wherein remediating the computer system includes performing supplemental remediations if the physical communication link is detached and subsequently attached.

37. (Previously presented) The method of claim 1, wherein remediating the computer system includes performing remediations scheduled for the computer system subsequent to the computer system disconnecting from the computer network.

38. (Previously presented) The method of claim 1, wherein determining if the computer system requires remediation includes determining if the computer system has any pending remediations.

39. (Previously presented) The method of claim 5, wherein a specified permitted communication between the computer system and the component of the network includes information needed for the computer system and the computer network to confirm that the computer system is attempting to re-enter its home network.

40. (Previously presented) The method of claim 5, wherein a specified permitted communication between the computer system and the component of the network includes information identifying the computer system and the component of the network.

41. (Previously presented) The method of claim 10, wherein limiting exchanges between said remediated computer network and said computer system includes allowing traffic needed for the computer system and the computer network to confirm

that the computer system is attempting to re-enter its home network and allowing other remediation related traffic between the client remediation server and the computer system.

42. (Previously presented) The method of claim 10, wherein limiting exchanges between said remediated computer network and said computer system includes allowing traffic needed to identify the computer system and the client remediation server and allowing other remediation related traffic between the client remediation server and the computer system.

43. (Previously presented) The method of claim 14, wherein the initiation of the connection is responsive to a physical communication link being connected between said computer system and said computer network subsequent to the communication link being disconnected.

44. (Previously presented) The method of claim 14, wherein said quarantine of said computer system is lifted upon said component of said computer network further completing an execution of any pending remediations for said computer system.

45. (Previously presented) The method of claim 14, wherein lowering the firewall generally permits all traffic to pass between said computer system and said remediated computer network without filtering by the firewall.